A Primer on the Federal Wiretap Act and Its Fourth Amendment Framework

By Daniel E. Monnat and Anne L. Ethen

I. Introduction

Recent law enforcement activity in this federal jurisdiction suggests that criminal defense attorneys may be encountering the fruits of federal wiretaps with greater frequency.[1] At first glance, the federal statutes governing wiretaps[2] may seem a disjointed and confusing set of special rules. However, for purposes of recognizing issues to litigate, it may be helpful to view wiretaps through the familiar framework of the Fourth Amendment. If the wiretap procedure is viewed as one which culminates in just another search warrant, many of the issues will be familiar from other search and seizure contexts.

It may be helpful to view wiretaps through the familiar framework of the Fourth Amendment.

II. The Fourth Amendment, the *Berger* Case & Title III

The Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[3]

In the early wiretapping and eavesdropping cases, there was much discussion of whether an interception without a physical invasion of property constituted a "search" within the meaning of the Fourth Amendment. Hence, in 1928 in *Olmstead v. United States*,[4] the United States Supreme Court permitted federal officers to wiretap suspected bootleggers without court supervision because the Fourth Amendment did not apply unless the G-men physically invaded the defendant's premises.[5]

Forty years later, by the time of *Berger v. New York*,[6] the United States Supreme Court had abandoned property law concepts and determined that the requirements of the Fourth Amendment should be applied to any statutory scheme purporting to authorize the search of wire communications:

> New York's broadside authorization rather than being "carefully circumscribed" so as to prevent unauthorized invasions of privacy actually permits general searches by electronic devices….[7]

Thus, in *Berger*, the Court struck down the eavesdropping statutory scheme of the State of New York for its failure to comply with the Fourth Amendment.[8]

The Court in *Berger* identified the following requirements for an inter-

Daniel E. Monnat *of Monnat & Spurrier, Chtd., has been a practicing criminal defense lawyer for the past 28 years in his hometown of Wichita, Kan. A cum laude graduate of California State University, San Francisco, he received his J.D. from the Creighton University School of Law. Monnat frequently lectures throughout the U.S. on criminal defense topics and has been listed in* The Best Lawyers in America *for the past decade. He is a past two-term president of the Kansas Association of Criminal Defense Lawyers, a member of the KTLA Board of Governors and Executive Committee, a graduate of the Gerry Spence Trial Lawyer's College, a member of the Board of Directors of the National Association of Criminal Defense Lawyers and a Fellow of the American College of Trial Lawyers.*

Anne L. Ethen *is an associate with Monnat & Spurrier, Chtd., in Wichita. She earned her undergraduate degree in economics from the University of Kansas, where she was selected for membership in Phi Beta Kappa. She received her J.D. from the University of Kansas School of Law, where she was a member of the Kansas Law Review, Order of the Coif and a Legal Research and Writing instructor. Following law school, Ethen worked as a law clerk for many years for the Hon. Frank G. Theis of the U.S. District Court for the District of Kansas. Ms. Ethen heads the research and writing division of Monnat & Spurrier.*

ception order to be constitutional under the Fourth Amendment: (1) there must be probable cause to believe that a particular offense has been or is being committed; (2) the conversations to be intercepted must be particularly described; (3) the surveillance must be for a specific, limited period of time; (4) if the warrant is to be renewed, continuing probable cause must be shown; (5) surveillance must terminate once the conversation sought has been seized; (6) notice must be provided unless a factual showing of exigency is made; and (7) a return must be made on the warrant so the court may supervise and restrict the use of the seized conversations.[9]

One year after the decision in *Berger*, Congress passed the Omnibus Crime Control and Safe Streets Act of 1968,[10] Title III of which enacted the statutory wiretapping scheme found in 18 U.S.C. § 2510 *et seq*. In that Act, Congress sought to enact a statutory wiretapping scheme that satisfied the Fourth Amendment requirements announced in *Berger*.

III. Probable Cause

Because of the Fourth Amendment requirement that no warrant shall issue but upon probable cause, supported by oath or affirmation, the wiretap procedure is, in many respects, like any other search warrant procedure. There must be a sworn application for this type of warrant,[11] based upon which the court issues an order for interception.[12]

However, a wiretap requires special judicial and executive authorization. An application for interception may not be filed unless it is first authorized by the attorney general or a specially designated deputy or assistant.[13] The application must identify the officer authorizing the application.[14] Attached to the government's application should be the authorization, as well as copies of the attorney general's designations of those Department of Justice officials who have been authorized to approve wiretaps.

Unlike traditional search warrants, a federal magistrate judge is not authorized to issue a wiretap. Only a federal district or circuit court judge may issue a wiretap.[15]

The application must contain a full and complete statement of the facts and circumstances relied upon to support a belief that an interception order should issue.[16] The issuing judge must determine that there exists probable cause to believe that particular communications concerning the alleged offenses will be obtained through interceptions of communications.[17]

In the usual search warrant case, probable cause includes two components: (1) that there is probable cause to believe that the items sought to be seized are connected with criminal activity; and (2) that the items sought to be seized will probably, presently be found in the place sought to be searched. In the wiretap context, before an interception order may issue, the judge must find: (1) probable cause for belief that a particular enumerated offense is being committed;[18] and (2) probable cause for belief that particular communications concerning that offense will be obtained through interception.[19]

Besides a sufficient factual predicate like probable cause, the Fourth Amendment requires that every search be "reasonable."[20] As with any other search, whether an electronic search is reasonable depends upon balancing the degree of intrusion against the need for it.[21] Thus, because an order to surreptitiously intercept private conversations is such an intrusive search, the application for interception must show more than mere probable cause, it must also show "necessity": the application must contain a full and complete statement as to whether other investigative procedures have been tried and failed or the reasons why such procedures reasonably appear to be unlikely to succeed or to be too dangerous if tried.[22] The issuing judge must find that normal investigative procedures have been tried and failed or reasonably appear unlikely to succeed or to be too dangerous if attempted.[23]

In the Tenth Circuit, the application must show that the following investigative methods have been tried and failed, or reasonably appear unlikely to succeed or to be too dangerous if attempted: (1) standard visual and aural surveillance; (2) questioning and interrogation of witnesses or participants (including the use of grand juries and grants of immunity); (3) use of search warrants; (4) infiltration of conspiratorial groups by undercover agents or informants; (5) pen registers or trap and trace devices; and (6) reviewing public, private, or governmental records pertaining to the suspects under investigation.[24]

Similarly, the application must fully disclose all previous applications for interception.[25] An application for an extension of a wiretap must contain a statement setting forth the results thus far obtained from the interception, or a reasonable explanation for the failure to obtain results.[26]

IV. The Particularity Requirement

By its terms, the Fourth Amendment requires that any search warrant particularly describe the place sought to be searched and the items sought to be seized. This particularity requirement applies in the case of a wiretap. There are a number of particularity requirements in the Wiretap Act.

A wiretap may issue only for particular crimes.[27] The application must contain a full and complete statement regarding the details as to the particular offense that has been, is being, or is about to be committed.[28] The issuing judge must find probable cause to believe those particular crimes are being committed, have been committed, or are about to be committed by an individual.[29]

The identities of persons to be intercepted must be particularly described in the application and order.[30] The nature and location of the communication facilities to be intercepted must be particularly set forth in the application and order.[31]

The application must contain a particular description of the type of communications sought to be intercepted.[32] The issuing judge must determine that there exists probable cause to believe that particular communications concerning the alleged offenses will be obtained through interceptions of communications.[33] The application and order must set forth either that interception will cease after the particular communication sought is first intercepted or that interception will continue for a particular time period.[34]

The purpose of this particularity

Continued on page 14

requirement of the Fourth Amendment is to prevent the execution of the overbroad "'general warrant' abhorred by the colonists" and the resulting "general, exploratory rummaging in a person's belongings."[35]

Given the intrusive nature of an interception order, the Wiretap Act incorporates a number of provisions which circumscribe the scope of the warrant and guard against law enforcement officers generally rummaging through phone calls.

The order for interception must contain a provision requiring the officers to execute the order in a manner whereby the interception of calls not particularly described and not otherwise subject to interception will be minimized.[36]

Similarly, no order may be entered authorizing interception for a period of time longer than necessary to achieve the objective, but in no event shall the authorization exceed 30 days.[37]

V. Scope & Execution Reasonableness

"[A] search which is reasonable at its inception may violate the Fourth Amendment by virtue of its intolerable intensity and scope."[38] This is the execution corollary of the Fourth Amendment's particularity requirement. The actual manner in which the interception order is executed must be examined to determine if the officers exceeded its scope and, by their actions, converted it into a general warrant.

Each order for interception must contain a provision that the authorization to intercept shall be executed as soon as practicable.[39] An initial fact investigation is necessary to determine compliance with this limitation on the intercept's scope.

More importantly, Congress has mandated that the contents of intercepted communications shall, if possible, be recorded.[40] The recording must be done in a manner to protect the recording from editing or alterations.[41]

These wiretap tape recordings, along with the transcripts and monitoring logs,[42] should be examined to determine whether the officers actually and effectively minimized or, rather, exceeded the scope of the interception authorized.

Likewise, if the interception order directs that the tap cease once the information sought is acquired, the tape recordings should be examined to determine whether the officers continued the tap beyond the temporal scope of the court's order.

VI. Post-Execution Reasonableness: Notice, Inventory & Return

When a home is searched pursuant to a warrant, the Fourth Amendment requires that the homeowner be given some notice at the time of the search and, thereafter, that an inventory and return be filed with the court. In essence, the same is required of a wiretap.

While advance notice of a wiretap would defeat its purposes, the government is required to ultimately provide notice. After the termination of interception, an inventory shall be served on the persons named in the application and order and the persons actually intercepted, giving notice of: (1) the fact of the entry of the order; (2) the date of the entry of the order and the period of authorized interception; and (3) the fact that during the period, communications were or were not intercepted.[43]

In the ordinary search warrant case, after execution of the warrant, the officer would prepare an inventory of the items seized and return that list to the judge. The property itself would not be submitted to the judge.

However, in wiretap cases, the items seized (i.e., the recorded conversations) are physically submitted to the judge. The tape recordings of intercepted calls must be made available to the judge immediately upon the expiration of the period of the order, and the tapes must be sealed in accordance with the judge's directions.[44]

If the tape recordings have not been sealed and the government does not provide a satisfactory explanation for the failure to seal, the contents of the intercepted communications and evidence derived therefrom may not be used or disclosed at trial.[45]

VII. Suppression, Standing & "Good Faith"

Strictly speaking, a motion to suppress the fruits of a wiretap should not be brought under the Fourth Amendment alone. The Wiretap Act contains its own exclusionary rule:

> Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence…if the disclosure of that information would be in violation of this chapter.[46]

Any person who was a party to an intercepted communication or a person against whom the interception was directed is an "aggrieved person"[47] under the Wiretap Act, and may move to suppress the contents of any intercepted communication and evidence derived therefrom.[48]

Not all violations of provisions of the Wiretap Act necessitate application of the exclusionary rule. Rather, only those provisions intended to play a central role in the statutory scheme require suppression:

> …we think Congress intended to require suppression where there is a failure to satisfy any of those statutory requirements that directly and substantially implement the congressional intention to limit the use of intercept procedures to those situations clearly calling for the employment of this extraordinary investigative device.[49]

To date, grounds for suppression include: (1) facial insufficiency of the orders, [50] (2) failure to demonstrate necessity,[51] (3) false or misleading statements in the application,[52] (4) minimization issues,[53] and (5) sealing issues.[54]

The question remains whether the good-faith exception to the exclusionary rule of *United States v. Leon*[55] applies in wiretap cases. The Tenth Circuit declined in *United States v. Castillo-Garcia*[56] to reach the question of whether a good-faith exception might apply to permit the admission of wiretap evidence obtained pursuant to a facially valid interception order issued in violation of the necessity requirement of the wiretap statute.[57] Subsequently, the court noted that it was an unsettled question whether the *Leon* good-faith exception applies in the wiretap context.[58]

Assuming that *Leon* would apply in wiretap cases, the Tenth Circuit has stated that it would not apply when

"the agent fails to meet Title III's requirements for applications and orders authorizing wiretaps."[59]

VIII. Conclusion

It is hoped that the initially daunting calculus of the federal Wiretap Act may be overcome by criminal defense attorneys instead viewing it, as here, through the Fourth Amendment's familiar framework of standing, probable cause, particularity, execution and post-execution reasonableness, "good faith" and suppression. ❖

Endnotes

[1] *E.g.*, *United States v. Garcia*, 02-10140-MLB (D. Kan.); *United States v. Hernandez-Sendejas*, 02-10117-WEB (D. Kan.); *United States v. Wright*, 00-40024-SAC (D. Kan.).

[2] Omnibus Crime Control and Safe Streets Act of 1968, Title III, Pub. L. No. 90-351, 82 Stat. 197 (1968), *codified at* 18 U.S.C. § 2510 *et seq*. For convenience of reference herein, the act will be referred to as the "Wiretap Act" or "Title III."

[3] U.S. Const. amend. IV.

[4] 277 U.S. 438 (1928).

[5] *Olmstead*, 277 U.S. at 466.

[6] 388 U.S. 41 (1967).

[7] *Berger*, 388 U.S. at 58.

[8] *Berger*, 388 U.S. at 58-59.

[9] *Berger*, 388 U.S. at 58-60.

[10] Pub. L. No. 90-351, 82 Stat. 197 (1968).

[11] 18 U.S.C. § 2518(1).

[12] 18 U.S.C. § 2518(3).

[13] 18 U.S.C. § 2516(1).

[14] 18 U.S.C. § 2518(1)(a).

[15] 18 U.S.C. §§ 2510(9) (defining "judge of competent jurisdiction"), 2516(1)&(3).

[16] 18 U.S.C. § 2518(1)(b).

[17] 18 U.S.C. § 2518(3)(b).

[18] 18 U.S.C. § 2518(3)(a).

[19] 18 U.S.C. § 2518(3)(b).

[20] The Fourth Amendment only prohibits "unreasonable" searches and seizures. U.S. Const. amend. IV; *see also Scott v. United States*, 436 U.S. 128 (1978) (discussing reasonableness as it applies to wiretaps).

[21] *Terry v. Ohio*, 392 U.S. 1, 21 (1968); *Scott v. United States*, 436 U.S. 128, 137 (1978); *United States v. Edwards*, 69 F.3d 419, 429 (10th Cir. 1995) (intrusive device of wiretapping not to be resorted to when traditional investigative techniques would suffice to expose the crime).

[22] 18 U.S.C. § 2518(1)(c).

[23] 18 U.S.C. § 2518(3)(c).

[24] *United States v. Castillo-Garcia*, 117 F.3d 1179, 1187-88 (10th Cir. 1997), *overruled on other grounds by United States v. Ramirez-Encarnacion*, 291 F.3d 1219, 1222 n. 1 (10th Cir. 2002).

[25] 18 U.S.C. § 2518(1)(e).

[26] 18 U.S.C. § 2518(1)(f).

[27] 18 U.S.C. § 2516.

[28] 18 U.S.C. § 2518(1)(b)(i).

[29] 18 U.S.C. § 2518(3)(a).

[30] 18 U.S.C. § 2518(1)(b)(iv), 2518(4)(a).

[31] 18 U.S.C. § 2518(1)(ii), 2518(4)(b).

[32] 18 U.S.C. § 2518(1)(b)(iii).

[33] 18 U.S.C. § 2518(3)(b).

[34] 18 U.S.C. § 2518(1)(d), 2518(4)(e).

[35] *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971).

[36] 18 U.S.C. § 2518(5).

[37] 18 U.S.C. § 2518(5).

[38] *Terry v. Ohio*, 392 U.S. 1, 18 (1968).

[39] 18 U.S.C. § 2518(5).

[40] 18 U.S.C. § 2518(8)(a).

[41] 18 U.S.C. § 2518(8)(a).

[42] A monitoring log is a written record of each telephone call and recording. The log sheet will normally identify: the cassette number upon which the telephone call is recorded; the call number; the agent who monitored the conversation; the date and time of the call; whether the call was incoming or outgoing; any caller ID and/or subscriber information; whether the call was fully recorded or minimized; the names of the parties to the conversation, if known; and whether the conversation was considered pertinent to the investigation. Additionally, the log sheet normally includes a summary of the conversation monitored.

[43] 18 U.S.C. § 2518(8)(d).

[44] 18 U.S.C. § 2518(8)(a).

[45] 18 U.S.C. § 2518(8)(a).

[46] 18 U.S.C.§ 2515.

[47] 18 U.S.C. § 2510(11).

[48] 18 U.S.C. § 2518(10)(a).

[49] *United States v. Giordano*, 416 U.S. 505, 527 (1974).

[50] 18 U.S.C. § 2518(10)(a)(ii).

[51] *See supra* text accompanying notes 22-24.

[52] *United States v. Green*, 175 F.3d 822, 828 (10th Cir. 1999).

[53] The government must make a prima facie showing of reasonable minimization. *United States v. Willis*, 890 F.2d 1099, 1102 (10th Cir. 1989). The court looks at the minimization efforts regarding the wiretap as a whole, and the minimization efforts regarding the particular defendant who seeks suppression on grounds of minimization. *Id*. As with most contemporary search and seizure issues, the subjective intention of the listening officer is largely irrelevant in determining whether proper minimization was conducted. *See Scott v. United States*, 436 U.S. 128 (1978).

[54] *See supra* text accompanying notes 44-45.

[55] 468 U.S. 897 (1984).

[56] 117 F.3d 1179 (10th Cir. 1997), *overruled on other grounds by United States v. Ramirez-Encarnacion*, 291 F.3d 1219, 1222 n. 1 (10th Cir. 2002).

[57] *Castillo-Garcia*, 117 F.3d at 1197.

[58] *See United States v. Arrington*, 2000 WL 775576, at ** 6 (10th Cir. June 16, 2000) (unpublished).

[59] *Arrington*, 2000 WL 775576, at ** 6.

Reprinted from the March 2004 issue of the Kansas Trial Lawyers Association Journal